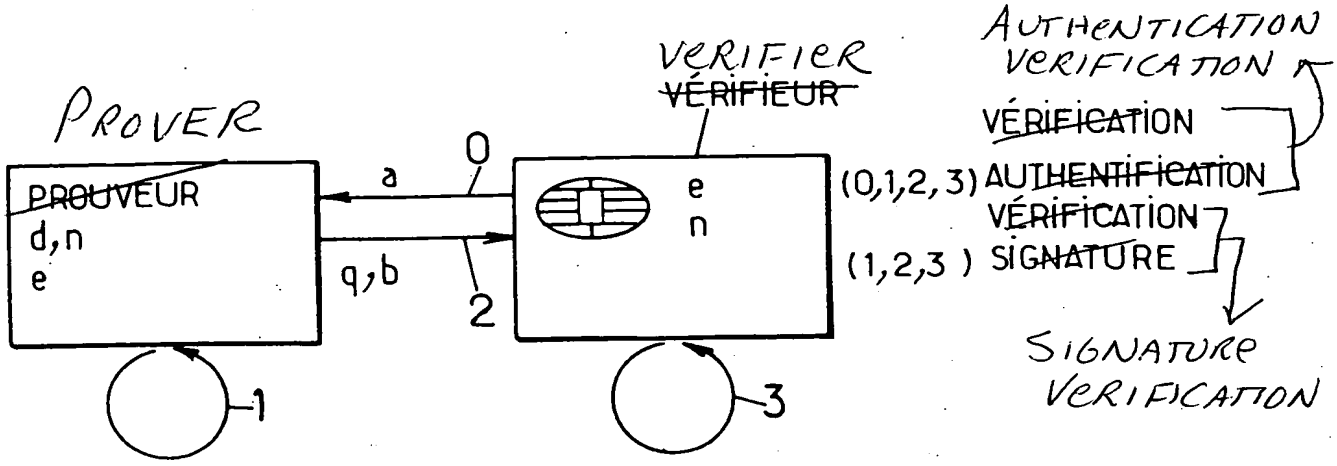



$q = a * b / n$

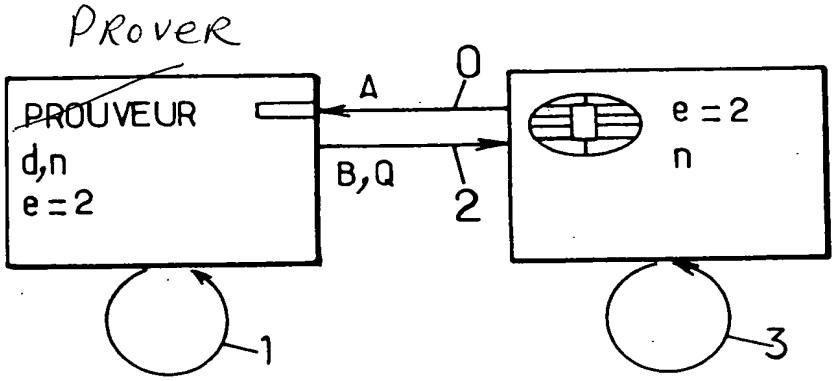
$b = \begin{cases} a^d \bmod n & \text{si } (0,1,2,3) \\ S = Sd(M) & \text{si } (1,2,3) \end{cases}$

$a * b$

$q * n$

$a * b - q * n$

FIG.1.




$R = B = A^d \bmod n$

$Q = B * B / n$

$D_{AR} = B * B - Q * n$

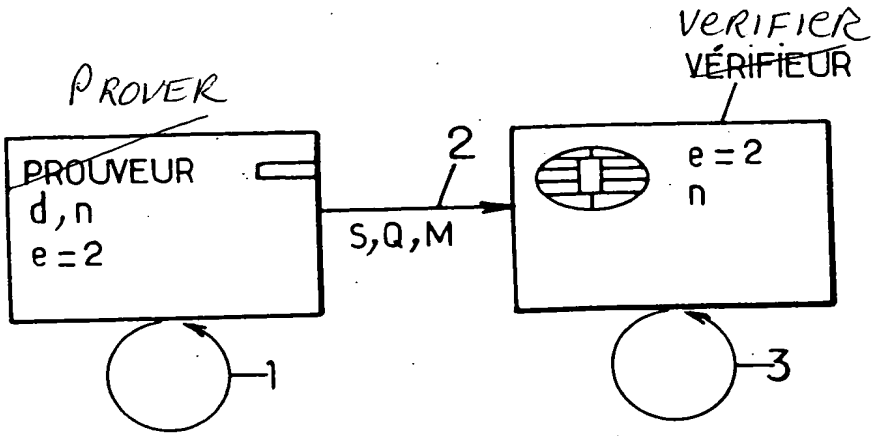
$D_{AR} = A$

$D_{AR} = n - A$

$D_{AR} = C * A \bmod n \} = C * A$ si $C * A < n$

$D_{AR} = -C * A \bmod n \} = C * A - n$ sinon

FIG. 2a.




VÉRIFICATION
SIGNATURE SIGNATURE
VERIFICATION

$R = S = Sd(M)$

$Q = S * S / n$

$D_{SR} = S * S - Q * n$

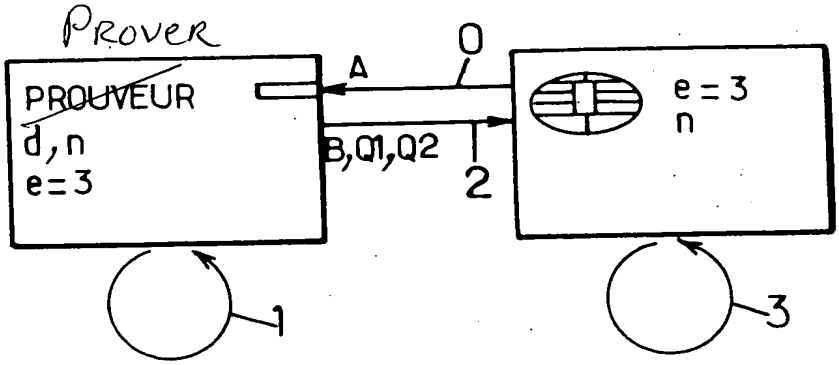
$D_{SR} = f(M)$

$= n - f(M)$

$= C * f(M) \bmod n = C * f(M)$ if $< n$

$= C * f(M) \bmod n = C * f(M)$ IF NOT

FIG.2b.




VÉRIFICATION
D'AUTHENTIFICATION
AUTHENTICATION
VERIFICATION

$R = B = A^d \bmod n$

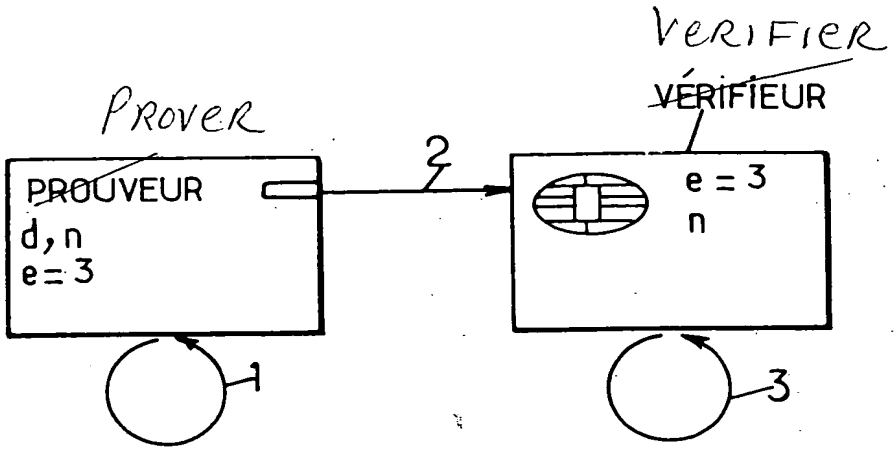
$Q1 = B * B / n$

$Q2 = B(B * B - Q1 * n) / n$

$D_{ARSA} = B(B * B - Q1 * n) - Q2 * n$

$D_{ARSA} = f(A) = A$

FIG.3a.




$R = S = Sd(M)$

$Q1 = S * S / n$

$Q2 = S(S * S - Q1 * n)/n$

$D_{SRSA} = S(S * S - Q1 * n) - Q2 * n$

$D_{SRSA} = f(M)$.

FIG.3b.